**Claims:**

1. (Currently Amended) A public-key encryption process for communicating messages between a sender and a receiver, comprising the steps of:

for each message:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver; ~~and~~

b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step, wherein the digital signature comprises a first value *r* and a second value *s*; and

~~wherein the ephemeral key pair used in the encrypting and generating steps is used for a single message between the sender and the receiver~~

c) transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;

wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X*, and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*.

2. (Original) A public-key encryption process according to claim 1, wherein the encrypting

step uses an El Gamal encryption scheme.

3. (Previously Presented) A public-key encryption process according to claim 1, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme;

wherein the step of generating the digital signature includes hashing the plaintext message.

4. (Currently Amended) A public-key encryption process according to claim 1, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key $x$ and calculating [[an]]the encryption ephemeral public key $X = xG$[[,]] in a finite cyclic group having ~~where~~ $G$ ~~is~~ as a generator.

5. (Original) A public-key encryption process according to claim 1, for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key $a$; and

b) calculating a sender public key $A = aG$, where $G$ is a generator,

and at the receiver,

a) generating a receiver private key $b$; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key $B$ and the receiver obtains an authentic copy of the sender public key $A$.

6. (Currently Amended) A public-key encryption process according to claim 5, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key $x$ and calculating [[an]]the encryption ephemeral public key $X = xG$.

7. (Original) A public-key encryption process according to claim 6, further comprising the steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key $K$ to generate a ciphertext message.

8. (Original) A public-key encryption process according to claim 7, further comprising the steps of, at the sender, using the encryption private key $x$ as a signature ephemeral private key and using the encryption ephemeral public key $X$ as a signature ephemeral public key to generate a digital signature.

9. (Cancelled)

10. (Currently Amended) A public-key encryption process according to claim ~~9~~8, further comprising the steps of, at the receiver, generating the secret key $K$ by calculating one of: ~~$= bX_x = bxG_x = xbG_x$~~ and ~~$= xB$~~[[,]] and decrypting the transmitted ciphertext message using the generated secret key $K$~~, calculating the first value $r$ of the digital signature using the decrypted message and the transmitted encryption ephemeral public key $X$ and validating the digital signature based on the calculated first value $r$ and the transmitted~~

~~second value s~~.

11. (Previously Presented) A public-key encryption process according to claim 1, implemented in a wireless communication system;

wherein at least a two stage public-key encryption process is used;

wherein the first stage includes key establishment and the second stage includes encryption/decryption;

wherein said steps (a) and (b) are performed during the second stage of encryption.

12. (Original) A public-key encryption process according to claim 1, implemented in a wireless hand-held communication device.

13. (Original) A public-key encryption process according to claim 1, implemented in a personal digital assistant.

14. (Original) A public-key encryption process according to claim 1, implemented in a cellular phone.

15. (Original) A public-key encryption process according to claim 1, implemented in a two-way pager.

16. (Currently Amended) A public-key encryption system for communicating messages between a sender and a receiver, comprising:

a) means, for each message, for encrypting a plaintext message into a ciphertext message, the means for encrypting producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver; ~~and~~

b) means, for each message, for generating a digital signature using the ephemeral key pair produced by the encrypting means, wherein the digital signature comprises a first value *r* and a second value *s*; and

~~wherein the ephemeral key pair used by the encrypting and generating means is used for a single message between the sender and the receiver~~

c) means for transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;

wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*.

17. (Original) A public-key encryption system according to claim 16, wherein the means for encrypting employs an E1 Gamal encryption scheme.

18. (Previously Presented) A public-key encryption system according to claim 16, wherein the means for generating a digital signature generates the digital signature using a Nyberg-Rueppel digital signature scheme.

19. (Currently Amended) A public-key encryption system according to claim 16, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating [[an]]the encryption ephemeral public key X = xG in a finite cyclic group having ~~where~~ G ~~is~~ as a generator.

20. (Original) A public-key encryption system according to claim 16, for encrypting messages for communication between a sender and a receiver, the system further comprising, at the sender,

a) means for generating a sender private key a; and

b) means for calculating a sender public key A = aG, where G is a generator, and at the receiver,

a) means for generating a receiver private key b; and

b) means for calculating a receiver public key B = bG,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains authentic copy of the sender public key A.

21. (Currently Amended) A public-key encryption system according to claim 20, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating [[an]]the encryption ephemeral public key X = xG.

22. (Original) A public-key encryption system according to claim 21, wherein the means for

encrypting generates a secret key K = xB and uses the secret key K to encrypt a plaintext message and thereby generate a ciphertext message.

23. (Previously Presented) A public-key encryption system according to claim 22, wherein the means for generating uses the encryption private key x as a signature ephemeral private key and uses the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

24. (Cancelled)

25. (Currently Amended) A public-key encryption system according to claim ~~24~~23, further comprising, at the receiver, means for decrypting a ciphertext message ~~and means for validating a digital signature~~, wherein the means for decrypting generates the secret key K = bX and decrypts the transmitted ciphertext message using the generated secret key K~~, and the means for validating calculates the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validates the digital signature based on the calculated first value r and the transmitted second value s~~.

26. (Original) A public-key encryption system according to claim 16, implemented in a wireless communication system.

27. (Original) A public-key encryption system according to claim 16, implemented in a

wireless hand-held communication device.

28. (Original) A public-key encryption system according to claim 16, implemented in a personal digital assistant.

29. (Original) A public-key encryption system according to claim 16, implemented in a cellular phone.

30. (Original) A public-key encryption system according to claim 16, implemented in a two-way pager.

31. (Currently Amended) A software program on a computer-readable storage medium, which when executed by a processor performs a public-key encryption process for communicating messages between a sender and a receiver comprising the steps of:

for each message:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver; ~~and~~

b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encryption step, wherein the digital signature comprises a first value $r$ and a second value $s$; and

~~wherein the ephemeral key pair used in the encrypting and generating steps is~~

~~used for a single message between the sender and the receiver~~

c) transmitting, from the sender, an encryption ephemeral public key $X$ of the ephemeral key pair, the ciphertext message, and the second value $s$ of the digital signature to the receiver;

wherein the first value $r$ of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key $X$ and validating the digital signature based on the calculated first value $r$ and the transmitted second value $s$;.

32. (Original) A software program according to claim 31, wherein the encrypting step uses an El Gamal encryption scheme.

33. (Previously Presented) A software program according to claim 31, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme.

34. (Currently Amended) A software program according to claim 31, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key $x$ and calculating [[an]]the encryption ephemeral public key $X = xG$, in a finite cyclic group having ~~where $G$ is~~ as a generator.

35. (Original) A software program according to claim 31, for encrypting messages for communication between a sender and a receiver, the software program performing the

further steps of, at the sender,

a) generating a sender private key $a$; and

b) calculating a sender public key $A = aG$, where $G$ is a generator,

and at the receiver,

a) generating a receiver private key $b$; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key $B$ and the receiver obtains an authentic copy of the sender public key $A$.

36. (Currently Amended) A software program according to claim 35, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key $x$ and calculating [[an]]the encryption ephemeral public key $X = xG$.

37. (Original) A software program according to claim 36, wherein the software program performs the further steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key $K$ to generate a ciphertext message.

38. (Original) A software program according to claim 37, wherein the software program performs the further steps of, at the sender, using the encryption private key $x$ as a signature ephemeral private key and using the encryption ephemeral public key $X$ as a signature ephemeral public key to generate a digital signature.

39. (Cancelled)

40. (Currently Amended) A software program according to claim ~~39~~38, the software program performing the steps of, at the receiver, generating the secret key $K$ by calculating one of: ~~$bX_s$ $bxG_s$ $xbG_s$ and $xB$~~[[,]]and decrypting the transmitted ciphertext message using the generated secret key ~~$K$ calculating the first value $r$ of the digital signature using the decrypted message and the transmitted encryption ephemeral public key $X$ and validating the digital signature based on the calculated first value $r$ and the transmitted second value $s$~~.

41. (Original) A software program according to claim 31, installed in a wireless communication system.

42. (Original) A software program according to claim 31, installed in a wireless hand-held communication device.

43. (Original) A software program according to claim 31, installed in a personal digital assistant.

44. (Original) A software program according to claim 31, installed in a cellular phone.

45. (Original) A software program according to claim 31, installed in a two-way pager.